



**CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. 1.8A)**

I hereby certify that this correspondence is, on the date shown below, being:

**MAILING**

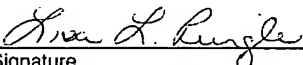
☒ deposited with the United States Postal Service in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450", as "Express mail post office to addressee" mailing label no. EB 027137118 US

**FACSIMILE**

☐ transmitted by facsimile to the Patent and Trademark Office @ (571)273-8300.

5 total number of pages.

Date: 4 January 2007

  
Signature  
Lisa L. Pringle  
(type or print name of person certifying)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: )  
Kenneth W. Aull ) Group Art Unit: 2137  
Serial No.: 10/027,622 ) Confirmation No.: 2941  
Filed: 19 December 2001 ) Examiner: Nadia Khoshnoodi  
For: *Assignment of User Certificates/Private Keys in Token Enabled Public Key Infrastructure System*

**PRE-APPEAL BRIEF REQUEST FOR REVIEW**

Mail Stop AF  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

In response to the Advisory Action filed in this case on November 27, 2006, please enter and consider the following remarks.

**Remarks/Arguments** begin on page 2 of this paper.

**REMARKS**

Claims 1-16 are currently pending in the subject application, and are presently under consideration. Claims 1-16 stand rejected by a Final Office Action issued October 6, 2006 ("Final Rejection") and an Advisory Action issued November 27, 2006. Favorable reconsideration of the application is requested in view of the comments herein.

**I. Rejection of Claims 1-6, 8-14 and 16 Under 35 U.S.C. §103(a)**

Claims 1-6, 8-14 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,192,131 to Geer, Jr. et al. ("Geer") in view of U.S. Patent No. 6,615,171 to Kanevsky et al. ("Kanevsky"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Geer taken in view of Kanevsky does not teach or suggest accessing a token through a token reader connected to a computer system by a certificate authority, as recited in claims 1 and 9. In a response filed to the Final Rejection, ("Final Response"), Applicant's representative clearly set forth reasons that Geer taken in view of Kanevsky does not teach or suggest this element of claims 1 and 9 (See Final Response, pages 2-3). Specifically, the section of Geer cited by the Examiner in the Final Rejection does not teach or suggest that a certifying authority (e.g., certificate authority) can access a smart card (e.g., token) at an authorizing computer 10. Instead, Geer discloses that a user is verified by the authorizing computer 10 sending an authorized computer 14 an identification certificate signed with the private key of the certifying authority, and the authorized computer 14 verifies the authenticity of the signature on the identification certificate (See Geer, Col. 2, Lines 50-60). That is, in claims 1 and 9, the certificate authority access the token, while in Geer, identity is verified by passing the identification certificate from the authorizing computer 10 to the authorized computer 14, and to the certifying authority. Accordingly, Geer taken in view of Kanevsky does not teach or suggest accessing a token through a token reader connected to a computer system by a certificate authority, as recited in claims 1 and 9.

Moreover, in the Final Response, Applicant's representative clearly set forth reasons that the Examiner failed to consider claims 1 and 9 *as a whole* (See Final Response, Pages 3-4). Specifically, when claims 1 and 9 are read as a whole, it is clear that a user-signature certificate is read and a certificate is downloaded to the same token, such that the token has two certificates, namely, the certificate and the user-signature certificate. Geer discloses that an authorizing computer 10 sends the authorized computer 14 a public key certificate (e.g., an identification certificate) identifying a user and the user's public key (See Geer, Col. 2, Lines 51-55). Assuming *arguendo* that an identification certificate is similar to a signature certificate, Geer still fails to teach or suggest the downloading recited in claims 1 and 9. The section of Geer that the Examiner contends discloses the downloading recited in claims 1 and 9, discloses that the authorizing computer 10 sends an authorization certificate to a smart card at the authorized computer 14 that interacts with a program stored at the authorized computer 14 (See Geer, Col.

6, Lines 7-10). That is, the smart card at the authorized computer 14 is a different smart card than the smart card from which the identification certificate is provided. Geer does not teach or suggest that the smart card at the authorized computer 14 contains an identification certificate, in contrast to the token recited in claims 1 and 9, which stores a signature certificate.

While Geer does disclose that the authorized computer 14 sends a public key certificate to the authorizing computer 10 for identifying the user of the authorized computer 14 (See Geer, Col. 2, Lines 60-63), Geer fails to teach or suggest that the public key certificate is ever stored on a smart card at the authorized computer 14, as suggested by the Examiner. In fact, the section of Geer that the Examiner contends discloses the downloading recited in claims 1 and 9 discloses that interaction with the smart card at the authorized computer 14 occurs when the authorized computer 14 contains a program that requires a license or a program fragment to function (See Geer, Col. 6, Lines 10-14). The cited section of Geer is not related to identification of the user of authorized computer 14. Thus, the sending of an authorization certificate to a smart card at the authorization computer 14 does not correspond to the downloading recited in claims 1 and 9. Accordingly, Geer taken in view of Kanevsky does not teach or suggest downloading a certificate and an associated private key to a token, when claims 1 and 9 are read as a whole.

Additionally, Applicant's representative agrees that Geer does not teach or suggest searching for a token ID and a user signature certificate from a token, searching for a match for the token ID and the user signature certificate in an authoritative database and that a certificate and an associated private key are wrapped with a public key associated with the token ID if a match is found for the token ID and the user signature certificate is found in the authoritative database, as recited in claims 1 and 9. However, in contrast to the contentions of the Examiner, the addition of Kanevsky does not make up for the deficiencies of Geer. In rejecting claims 1 and 9, the Examiner cites Col. 8, Lines 29-46 of Kanevsky (See Final Rejection, Pages 5-6). In the Final Response, Applicant's representative clearly set forth reasons that Geer taken in view of Kanevsky does not teach or suggest the searching recited in claims 1 and 9 (See Final Response, Pages 4-5). Specifically, the cited section of Kanevsky discloses that if a user forgets his personal identification number (PIN) or if his PIN expires without being reset that the user can reestablish his PIN by linking to an automatic speech/speaker recognition (ASSR) server 200 via a communication link to request a PIN reset through a personal computer (PC) 450 and a smart card reader 460 (See Kanevsky, Col. 8, Lines 21-28). Kanevsky does not teach or suggest that a certificate and an associated private key are wrapped with a public key associated with a token ID, as recited in claims 1 and 9. Instead, Kanevsky discloses that a PIN reset command is encrypted with a smart card's certificate and public key. Clearly, the PIN reset command does not correspond to the certificate recited in claims 1 and 9. Accordingly, taken individually or in combination, Geer and Kanevsky do not teach or suggest each and every element of claims 1 and 9.

Furthermore, in the Final Response, Applicant's representative clearly set forth reasons that there is no motivation to combine and modify the teachings of Geer and Kanevsky in the

manner suggested by the Examiner (See Final Response, Page 5). Specifically, Applicant's representative respectfully submits that if the system disclosed in Geer were modified to employ smart card IDs in the manner suggested by the Examiner, particular smart cards (e.g., tokens) would need to be assigned to particular users and computers in an authoritative database. That is, the smart cards would not be generic or transferable (e.g., by copying contents of the smart card). There is no motivation in Geer to employ such a system, as employing smart card IDs (e.g., token IDs) would result in a less convenient system. One skilled in the art would not be motivated to tradeoff the benefit of using a generic smart card for the increased security and complexity of a system where the smart cards were assigned to particular users and computers. Therefore, Geer taken in view of Kanevsky does not make claims 1 and 9 obvious, and claims 1 and 9, as well as claims 2-6, 8, 10-14 and 16 depending therefrom, should be patentable over the cited art.

Additionally, regarding claims 2 and 10, in the Final Response, Applicant's representative clearly set forth reasons that Greer taken in view of Kanevsky does not teach or suggest the elements recited in claims 2 and 10 (See Final Response, Page 6). Specifically, claims 2 and 10 defines properties of the certificate recited in claims 1 and 9 that is downloaded to a token. In rejecting claims 2 and 10, the Examiner cites Col. 3, Lines 29-33 of Geer. Geer discloses that an authorization certificate is generated by a smart card on an authorizing computer 10 (See Geer, Col. 3, Lines 23-24) and the smart card signs the authorization certificate with the private key of the smart card (See Geer Col. 3, Lines 33-34). Geer also discloses that the authorizing computer 10 sends the authorization certificate to a smart card at the authorized computer 14 (See Geer, Col. 6, Lines 8-10). However, since claims 2 and 10 depend from claims 1 and 9, respectively, the certificate recited in claims 2 and 10 is downloaded to the token, which is the same token from which a user signature certificate is read. For the reasons stated above, Geer taken in view of Kanevsky does not teach or suggest reading a token ID and a user-signature certificate from a token and downloading a certificate and associated private key to the same token, as recited in claims 1 and 9, from which claims 2 and 10 depend. Therefore, Geer taken in view Kanevsky does not teach or suggest specific properties of the certificate that is downloaded to the token, as recited in claims 2 and 10. Thus, Geer taken in view of Kanevsky not teach or suggest each and every element of claims 2 and 10.

For the reasons described above, claims 1-6, 8-14 and 16 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

## **II. Rejection of Claims 7 and 15 Under 35 U.S.C. §103(a)**

Claims 7 and 15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Geer and Kanevsky and further in view of U.S. Publication No. 2003/0005291 to Burn ("Burn"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 7 and 15 depend from claims 1 and 9, respectively. The further addition of Burn does not make up for the aforementioned deficiencies of Geer taken in view of Kanevsky, with respect to claims 1 and 9, from which claims 7 and 15 depend.

Additionally, in the Final Response, Applicant's representative clearly set forth reasons that Greer taken in view of Kanevsky and Burn teach away from their respective combination and modification in the manner suggested by the Examiner (See Final Response, pages 7-8). Specifically, in the Final Rejection, the Examiner contends that Kanevsky discloses several reasons for sending the PIN reset command (See Final Rejection, Page 4, citing Col. 8, Lines 21-31 of Kanevsky). However, in Kanevsky the only reasons taught or suggested for sending a PIN reset command, as discussed above with respect to claims 1 and 9, is when a user forgets his PIN or the PIN has expired (See Kanevsky, Col. 8, Lines 21-23). Claims 7 and 15 require that a passphrase be entered by a user. If the teachings of Geer and Kanevsky were combined and modified with Burn such that a user were required to enter a PIN when the user forgot his PIN or the PIN were expired, the user would not be able to decrypt the PIN reset command, since that user would not be able to remember his PIN, or the PIN would no longer be valid (e.g., expired). Accordingly, Applicant's representative respectfully submits that combining and modifying the teachings of Geer, Kanevsky and Burn in the manner suggested by the Examiner would result in an inoperable device, and thus, the references teach away from their combination. Thus, claims 7 and 15 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.


#### CONCLUSION

In view of the foregoing remarks, Applicant's representative respectfully submits that the present application is in condition for allowance. Applicant's representative respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 1-9-07

  
\_\_\_\_\_  
Christopher P. Harris  
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.  
1300 EAST NINTH STREET, SUITE 1700  
CLEVELAND, OHIO 44114  
Phone: (216) 621-2234  
Fax: (216) 621-4072